IN THE CLAIMS:

Amended claims follow:

1. (Currently Amended) A system for automatically protecting private video content using cryptographic security for legacy systems, comprising:

a transportable storage medium, comprising:

recording logic intercepting a substantially continuous video signal representing video content in the process of being recorded on a transportable storage medium;

a frame buffer dividing the intercepted substantially continuous video signal into individual frames during recording, each individual frame storing a fixed amount of data in digital form, and combining decrypted frames into a substantially continuous video signal during playback;

a processor encrypting each individual frame into encrypted video content using an encryption cryptographic key and storing the encrypted frames during recording and retrieving the encrypted frames and decrypting each encrypted frame using a decryption cryptographic key during playback;

reading logic outputting the substantially continuous video signal as video content in the process of being played from the transportable storage medium;

a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key, where the removable storage medium is removable with respect to the transportable storage medium;~~and~~

an authentication module generating a fixed-length original cryptographic hash from at least one such individual frame, encrypting the original cryptographic hash using an encryption cryptographic key, storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium, retrieving the digital signature from the transportable storage medium, decrypting the encrypted original cryptographic hash using a decryption cryptographic key, generating a verification fixed-length cryptographic hash from at least one such individual frame, and comparing the verification cryptographic hash and the original cryptographic hash; and

a validation module validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames;

wherein the removable storage medium includes memory that is coupled to a standardized connector which enables utilization of at least one of a plurality of encryption cryptographic keys and a plurality of decryption cryptographic keys.

2. (Cancelled)

3. (Previously Presented) A system according to Claim 1, further comprising:

an asymmetric cryptographic key pair comprising a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key.

4. (Cancelled)

5. (Original) A system according to Claim 1, further comprising:

an asymmetric cryptographic key pair comprising a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

6. (Original) A system according to Claim 5, wherein the asymmetric cryptographic key pair comprises at least one of an RSA-compatible key pair, a TwoFish-compatible key pair and a Diffie-Hellman-compatible key pair.

7. (Original) A system according to Claim 1, further comprising:

a symmetric cryptographic key pair comprising a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

8. (Cancelled)

9. (Previously Presented) A system according to Claim 1, further comprising:

a set of cryptographic instructions stored on the removable storage medium and employing at least one of the encryption cryptographic key and the decryption cryptographic key.

10. (Currently Amended) A method for automatically protecting private video content using cryptographic security for legacy systems, comprising:

intercepting a substantially continuous video signal representing video content in the process of being recorded on a transportable storage medium;

dividing the intercepted substantially continuous video signal into individual frames which each store a fixed amount of data in digital form;

encrypting each individual frame into encrypted video content using an encryption cryptographic key and storing the encrypted frames;

retrieving encrypted frames and decrypting each encrypted frame using a decryption cryptographic key;

combining the decrypted frames into a substantially continuous video signal;

outputting the substantially continuous video signal as video content in the process of being played from the transportable storage medium;

storing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium, where the removable storage medium is removable with respect to the transportable storage medium;

generating a fixed-length original cryptographic hash from at least one such individual frame;

encrypting the original cryptographic hash using an encryption cryptographic key and storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium;

retrieving the digital signature from the transportable storage medium and decrypting the encrypted original cryptographic hash using a decryption cryptographic key;

generating a verification fixed-length cryptographic hash from at least one such individual frame and comparing the verification cryptographic hash and the original cryptographic hash;~~-and~~

outputting the substantially continuous video signal upon successful comparison of the verification cryptographic hash and the original cryptographic hash; and

validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames;

wherein the removable storage medium includes memory that is coupled to a standardized connector which enables utilization of at least one of a plurality of encryption cryptographic keys and a plurality of decryption cryptographic keys.

11. (Cancelled)

12. (Previously Presented) A method according to Claim 10, further comprising:

providing an asymmetric cryptographic key pair comprising a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key.

13. (Cancelled)

14. (Original) A method according to Claim 10, further comprising:

providing an asymmetric cryptographic key pair comprising a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

15. (Original) A method according to Claim 14, wherein the asymmetric cryptographic key pair comprises at least one of an RSA-compatible key pair, a TwoFish-compatible key pair and a Diffie-Hellman-compatible key pair.

16. (Original) A method according to Claim 10, further comprising:

providing a symmetric cryptographic key pair comprising a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

17. (Cancelled)

18. (Previously Presented) A method according to Claim 10, further comprising:

including a set of cryptographic instructions employing at least one of the encryption cryptographic key and the decryption cryptographic key on the removable storage medium.

19. (Currently Amended) A computer-readable storage medium holding code for performing the method according to Claims 10, 12, [13, ]14, 16 or 18.

20. (Currently Amended) A system for encrypting private video content using cryptographic security for legacy systems, comprising:

recordation logic intercepting a substantially continuous video signal prior to recordation on a transportable storage medium, the signal representing raw video content;

a frame buffer dividing the signal into individual frames which each store a fixed amount of data in digital form;

a processor encrypting each individual frame into encrypted video content using an encryption key selected from a cryptographic key pair and storing the encrypted frames on the transportable storage medium for retrieval and decryption using a decryption key selected from the cryptographic key pair, the processor generating a fixed-length original cryptographic hash from at least one such individual frame, encrypting the original cryptographic hash using an encryption cryptographic key from a cryptographic key pair, and storing the encrypted original cryptographic hash as a digital

signature on the transportable storage medium for retrieval and decryption using a decryption key selected from the cryptographic key pair;~~-and~~

a removable storage medium storing at least one of the encryption key and the decryption key, where the removable storage medium is removable with respect to the transportable storage medium; and

a validation module validating the decryption key against user-provided credentials prior to decrypting the encrypted frames;

wherein the removable storage medium includes memory that is coupled to a standardized connector which enables utilization of at least one of a plurality of encryption keys and a plurality of decryption keys.

21. (Cancelled)

22. (Previously Presented) A system according to Claim 20, further comprising:

a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key.

23. (Original) A system according to Claim 20, further comprising:

a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

24. (Original) A system according to Claim 20, further comprising:

a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

25. (Cancelled)

26. (Currently Amended) A method for encrypting private video content using cryptographic security for legacy systems, comprising:

intercepting a substantially continuous video signal prior to recordation on a transportable storage medium, the signal representing raw video content, and dividing the signal into individual frames which each store a fixed amount of data in digital form;

encrypting each individual frame into encrypted video content using an encryption key selected from a cryptographic key pair;

storing the encrypted frames on the transportable storage medium for retrieval and decryption using a decryption key selected from the cryptographic key pair;~~-and~~

storing at least one of the encryption key and the decryption key on a removable storage medium, where the removable storage medium is removable with respect to the transportable storage medium;

generating a fixed-length original cryptographic hash from at least one such individual frame;

encrypting the original cryptographic hash using an encryption cryptographic key from a cryptographic key pair;~~-and~~

storing the encrypted original cryptographic hash as a digital signature on the transportable storage medium for retrieval and decryption using a decryption key selected from the cryptographic key pair; and

validating the decryption key against user-provided credentials prior to decrypting the encrypted frames;

wherein the removable storage medium includes memory that is coupled to a standardized connector which enables utilization of at least one of a plurality of encryption cryptographic keys and a plurality of decryption keys.

27. (Cancelled)

28. (Previously Presented) A method according to Claim 26, further comprising:

employing a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key.

29. (Original) A method according to Claim 26, further comprising:

employing a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

30. (Original) A method according to Claim 26, further comprising:

employing a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

31. (Cancelled)

32. (Previously Presented) A computer-readable storage medium holding code for performing the method according to Claims 26, 28, 29 or 30.

33. (Currently Amended) A system for decrypting private video content using cryptographic security for legacy systems, comprising:

reading logic retrieving encrypted frames prior to playback from a transportable storage medium, the encrypted frames storing raw video content encrypted using an encryption cryptographic key selected from a cryptographic key pair;

a processor decrypting each encrypted frame using a decryption cryptographic key selected from the cryptographic key pair;

a frame buffer combining the decrypted frames into a substantially continuous video signal representing the raw video content in reconstructed form; and

a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key, where the removable storage medium is removable with respect to the transportable storage medium;

the reading logic retrieving a digital signature included with the encrypted frames and encrypted using an encryption cryptographic key selected from a cryptographic key pair;

the processor generating a verification fixed-length cryptographic hash from at least one such individual frame and comparing the verification cryptographic hash and the original cryptographic hash; ~~and~~

the frame buffer combining the individual frames into a substantially continuous video signal and outputting the substantially continuous video signal as video content in the process of being played from the transportable storage medium upon successful comparison of the verification cryptographic hash and the original cryptographic hash; and

a validation module validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames;

wherein the removable storage medium includes memory that is coupled to a standardized connector which enables utilization of at least one of a plurality of encryption cryptographic keys and a plurality of decryption cryptographic keys.

34. (Cancelled)

35. (Cancelled)

36. (Original) A system according to Claim 33, further comprising:

a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

37. (Original) A system according to Claim 33, further comprising:

a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

38. (Cancelled)

39. (Currently Amended) A method for decrypting private video content using cryptographic security for legacy systems, comprising:

retrieving encrypted frames prior to playback from a transportable storage medium, the encrypted frames storing raw video content encrypted using an encryption cryptographic key selected from a cryptographic key pair;

decrypting each encrypted frame using a decryption cryptographic key selected from the cryptographic key pair;

combining the decrypted frames into a substantially continuous video signal representing the raw video content in reconstructed form;

storing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium, where the removable storage medium is removable with respect to the transportable storage medium;

retrieving a digital signature included with the encrypted frames and encrypted using an encryption cryptographic key selected from a cryptographic key pair;

generating a verification fixed-length cryptographic hash from at least one such individual frame and comparing the verification cryptographic hash and the original cryptographic hash;~~-and~~

combining the individual frames into a substantially continuous video signal and outputting the substantially continuous video signal as video content in the process of being played from the transportable storage medium upon successful comparison of the verification cryptographic hash and the original cryptographic hash; and

validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames;

wherein the removable storage medium includes memory that is coupled to a standardized connector which enables utilization of at least one of a plurality of encryption cryptographic keys and a plurality of decryption cryptographic keys.

40. (Cancelled)

41. (Cancelled)

42. (Original) A method according to Claim 39, further comprising:

employing a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

43. (Original) A method according to Claim 39, further comprising:

employing a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

44. (Cancelled)

45. (Previously Presented) A computer-readable storage medium holding code for performing the method according to Claims 39, 42 or 43.

46. (Currently Amended) A method for automatically authenticating private video content using cryptographic security for legacy systems, comprising:

a transportable storage medium, comprising:

recording logic intercepting a substantially continuous video signal representing video content in the process of being recorded on a transportable storage medium;

a frame buffer dividing a substantially continuous video signal representing raw video content into individual frames which each store a fixed amount of data in digital form and combining the individual frames into a substantially continuous video signal;

a processor generating a fixed-length original cryptographic hash from at least one such individual frame, encrypting the original cryptographic hash using an encryption cryptographic key, storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium, retrieving the digital signature from the transportable storage medium, decrypting the encrypted original cryptographic hash using a decryption cryptographic key, generating a verification fixed-length cryptographic hash from at least one such individual frame, and comparing the verification cryptographic hash and the original cryptographic hash;

reading logic outputting the substantially continuous video signal as video content in the process of being played from the transportable storage medium upon successful

comparison of the verification cryptographic hash and the original cryptographic hash; ~~and~~

a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key, where the removable storage medium is removable with respect to the transportable storage medium; and

a validation module validating the decryption cryptographic key against user-provided credentials prior to decrypting encrypted frames;

wherein the removable storage medium includes memory that is coupled to a standardized connector which enables utilization of at least one of a plurality of encryption cryptographic keys and a plurality of decryption cryptographic keys.

47.-49. (Cancelled)

50. (Previously Presented) A system according to Claim 46, further comprising:

a set of cryptographic instructions employing at least one of the encryption cryptographic key and the decryption cryptographic key on the removable storage medium.

51. (Currently Amended) A method for automatically authenticating private video content using cryptographic security for legacy systems, comprising:

intercepting a substantially continuous video signal representing video content in the process of being recorded on a transportable storage medium;

dividing a substantially continuous video signal representing raw video content into individual frames which each store a fixed amount of data in digital form;

generating a fixed-length original cryptographic hash from at least one such individual frame;

encrypting the original cryptographic hash using an encryption cryptographic key and storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium;

retrieving the digital signature from the transportable storage medium and decrypting the encrypted original cryptographic hash using a decryption cryptographic key;

generating a verification fixed-length cryptographic hash from at least one such individual frame and comparing the verification cryptographic hash and the original cryptographic hash;

combining the individual frames into a substantially continuous video signal and outputting the substantially continuous video signal as video content in the process of being played from the transportable storage medium upon successful comparison of the verification cryptographic hash and the original cryptographic hash;~~-and~~

storing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium, where the removable storage medium is removable with respect to the transportable storage medium; and

validating the decryption cryptographic key against user-provided credentials prior to decrypting encrypted frames;

wherein the removable storage medium includes memory that is coupled to a standardized connector which enables utilization of at least one of a plurality of encryption cryptographic keys and a plurality of decryption cryptographic keys.

52.-54. (Cancelled)

55. (Previously Presented) A method according to Claim 51, further comprising:

including a set of cryptographic instructions employing at least one of the encryption cryptographic key and the decryption cryptographic key on the removable storage medium.

56. (Previously Presented) A computer-readable storage medium holding code for performing the method according to Claims 51 or 55.

57. (Currently Amended) A system for digitally signing private video content using cryptographic security for legacy systems, comprising:

recordation logic intercepting a substantially continuous video signal prior to recordation on a transportable storage medium, the signal representing raw video content;

a frame buffer dividing the signal into individual frames which each store a fixed amount of data in digital form;

a processor generating a fixed-length original cryptographic hash from at least one such individual frame, encrypting the original cryptographic hash using an encryption cryptographic key from a cryptographic key pair, and storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium for retrieval and decryption using a decryption key selected from the cryptographic key pair; ~~and~~

providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium, where the removable storage medium is removable with respect to the transportable storage medium; and

a validation module validating the decryption cryptographic key against user-provided credentials prior to decrypting encrypted frames;

wherein the removable storage medium includes memory that is coupled to a standardized connector which enables utilization of at least one of a plurality of encryption cryptographic keys and a plurality of decryption cryptographic keys.

58. (Cancelled)

59. (Original) A system according to Claim 57, further comprising:

employing a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

60. (Cancelled)

61. (Currently Amended) A method for digitally signing private video content using cryptographic security for legacy systems, comprising:

intercepting a substantially continuous video signal prior to recordation on a transportable storage medium, the signal representing raw video content;

dividing the signal into individual frames which each store a fixed amount of data in digital form;

generating a fixed-length original cryptographic hash from at least one such individual frame;

encrypting the original cryptographic hash using an encryption cryptographic key from a cryptographic key pair;

storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium for retrieval and decryption using a decryption key selected from the cryptographic key pair;~~-and~~

storing at least one of the encryption cryptographic key and the decryption key on a removable storage medium, where the removable storage medium is removable with respect to the transportable storage medium; and

validating the decryption key against user-provided credentials prior to decrypting encrypted frames;

wherein the removable storage medium includes memory that is coupled to a standardized connector which enables utilization of at least one of a plurality of encryption cryptographic keys and a plurality of decryption keys.

62. (Cancelled)

63. (Original) A method according to Claim 61, further comprising:

employing a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

64. (Cancelled)

65. (Previously Presented) A computer-readable storage medium holding code for performing the method according to Claims 61or 63.

66. (Currently Amended) A system for verifying digitally signed private video content using cryptographic security for legacy systems, comprising:

reading logic retrieving frames prior to playback from a transportable storage medium, the frames storing raw video content and including a digital signature encrypted using an encryption cryptographic key selected from a cryptographic key pair;

a processor generating a verification fixed-length cryptographic hash from at least one such individual frame and comparing the verification cryptographic hash and the original cryptographic hash;

a frame buffer combining the individual frames into a substantially continuous video signal and outputting the substantially continuous video signal as video content in the process of being played from the transportable storage medium upon successful comparison of the verification cryptographic hash and the original cryptographic hash; ~~and~~

a removable storage medium storing the encryption cryptographic key, where the removable storage medium is removable with respect to the transportable storage medium; and

a validation module validating a decryption cryptographic key against user-provided credentials prior to decrypting encrypted frames;

wherein the removable storage medium includes memory that is coupled to a standardized connector which enables utilization of at least one of a plurality of encryption cryptographic keys and a plurality of decryption cryptographic keys.

67. – 68. (Cancelled)

69. (Currently Amended) A method for verifying digitally signed private video content using cryptographic security for legacy systems, comprising:

retrieving frames prior to playback from a transportable storage medium, the frames storing raw video content and including a digital signature encrypted using an encryption cryptographic key selected from a cryptographic key pair;

generating a verification fixed-length cryptographic hash from at least one such individual frame and comparing the verification cryptographic hash and the original cryptographic hash;

combining the individual frames into a substantially continuous video signal and outputting the substantially continuous video signal as video content in the process of being played from the transportable storage medium upon successful comparison of the verification cryptographic hash and the original cryptographic hash; ~~and~~

storing the encryption cryptographic key on a removable storage medium, where the removable storage medium is removable with respect to the transportable storage medium; and

validating a decryption cryptographic key against user-provided credentials prior to decrypting encrypted frames;

wherein the removable storage medium includes memory that is coupled to a standardized connector which enables utilization of at least one of a plurality of encryption cryptographic keys and a plurality of decryption cryptographic keys.

70. (Cancelled)

71. (Cancelled)

72. (Previously Presented) A computer-readable storage medium holding code for performing the method according to Claim 69.

73. (Cancelled)

74. (Previously Presented) The system according to Claim 1, wherein during the recording a first cryptographic hash is generated from at least one of the individual

frames utilizing a one-way hashing function and the at least one of the individual frames is encrypted utilizing the encryption cryptographic key.

75. (Previously Presented) The system according to Claim 74, wherein during the playback the first cryptographic hash is retrieved and decrypted utilizing the decryption cryptographic key.

76. (Previously Presented) The system according to Claim 75, wherein a second cryptographic hash is generated from the at least one of the individual frames and compared to the decrypted first cryptographic hash.

77. (Previously Presented) The system according to Claim 76, wherein the video content is played if the first cryptographic hash and the second cryptographic hash match.

78. (Previously Presented) The system according to Claim 1, wherein the removable storage medium is removably coupled to a video tape cassette.